CLAIMS

1. An apparatus (AG) arranged for receiving (S-23) an access request in a telecommunication core network (CN) from an entity (WLAN-AS) in an access network (WLAN) where a user with a user's equipment (UE) accesses through, the user being subscriber of the telecommunication core network (CN) and being identified by a user's identifier included in the access request, the apparatus having:

   - means for carrying out (S-25) an authentication procedure (SIM-based; AKA; EAP) with the user's equipment (UE) through the access network (WLAN) in order to authenticate the user; and

   - means for computing at least one secret user's key (K_c) usable as cryptographic material;

   and **characterised by** comprising:

   - means for deriving (S-251) from the cryptographic material a user's shared key (SSO_key-1) intended for SSO purposes; and

   - means for sending (S-30) the user's shared key (SSO_key-1) along with the user's identifier towards a session manager (SSO_SM) serving a service network (SN).

2. The apparatus of claim 1, further comprising means for being notified (S-29) that a session at the access level has been established, this notification triggering the sending (S-30) of the user's shared key (SSO_key-1) towards the session manager (SSO_SM) serving the service network (SN).

3. The apparatus of claim 2, further comprising means for being notified that a session at the access level has

been terminated (accounting stop message), and means for forwarding this notification towards the session manager (SSO_SM) serving the service network (SN) in order to inactivate a current master session for the user.

4. A session manager (SSO_SM) serving a service network (SN) for SSO purposes and arranged for managing a session record for a user accessing the service network (SN) through an access network (WLAN), the user having been authenticated by a telecommunication core network (CN) where the user holds a subscription, the session manager (SSO_SM) **characterised in that** comprises:

- means for receiving (S-30) a first user's shared key (SSO_key-1) and a user's identifier from the core network (CN) for SSO authentication purposes, this first user's shared key (SSO_key-1) obtainable during the authentication of the user by the core network (CN);

- means for creating (S-301) a master session for the user that comprises the user's identifier and the received first user's shared key (SSO_key-1); and

- means for checking (S-34) whether a second user's shared key (SSO_key-2) derived at the user's equipment (UE) matches the first user's shared key (SSO_key-1) included in the master session for the user.

5. The session manager of claim 4, further including means for creating a service session to index the master session, in case of matching first and second user's shared keys, this service session intended as a token of a successful SSO user authentication.

6. The session manager of claim 5, further including means for verifying whether a service session indexes an active

master session for a user to determine if a previous SSO authentication is still valid.

7. The session manager of claim 4, wherein the means for checking (S-34), whether a second user's shared key (SSO_key-2) derived at the user's equipment (UE) matches the first user's shared key (SSO_key-1) included in the master session, comprises means for processing the first user's shared key (SSO_key-1) to obtain a first key code (MAC(SSO_key-1)) to be matched against a second key code (MAC(SSO_key-2)) originated from the user's equipment.

8. An apparatus (SAAN) intended for receiving (S-31) a request from a user accessing a telecommunication service network (SN) through an access network (WLAN) with a user's equipment (UE), the user already authenticated by a telecommunication core network (CN) where the user holds a subscription, the request including a user's identifier to identify the user, the apparatus **characterised by** comprising:

- means for verifying whether an active service session is indicated in the request from the user's equipment;

- means for assessing (S-33) that a user's shared key (SSO_key-2) is stored in the user's equipment (UE); and

- means for determining (S-34) in cooperation with a session manager (SSO_SM) serving the service network (SN) for SSO purposes whether the user's shared key (SSO_key-2) at the user's equipment (UE) matches the one stored in the master session (SSO_key-1) for the user.

9. The apparatus of claim 8, further comprising means for obtaining a service session for a user from the session

manager (SSO_SM) serving the service network (SN) for SSO purposes.

10. The apparatus of claim 9, further including means for generating an SSO cookie to be submitted (S-37) to the user's equipment (UE), the SSO cookie comprising the service session.

11. The apparatus of claim 10, further comprising means for receiving an SSO cookie from the user's equipment (UE), the SSO cookie indicating a service session for the user.

12. The apparatus of claim 8, further comprising means for downloading an SSO plug-in towards the user's equipment, the SSO plug-in running for confirming back the user's shared key (SSO_key-2).

13. The apparatus of claim 8, wherein the means for assessing (S-33) that a user's shared key (SSO_key-2) is stored in the user's equipment (UE) includes means for receiving from the user's equipment an element selected from:

- a key code (MAC(SSO_key-2)) obtainable by processing the user's shared key (SSO_key-2) at the user's equipment; and

- the user's shared key (SSO_key-2).

14. The apparatus of claim 13, further comprising means for submitting the received element to a cooperating session manager (SSO_SM) serving the service network (SN) for SSO purposes.

15. A use of the apparatus of claim 8 as an HTTP Proxy receiving service requests (S-31) from users accessing a service network (SN) in a Walled-Garden SSO model.

16. A use of the apparatus of claim 8 as an authentication node of an Identity Provider where a credential request

(S-31) is received from a user accessing a service of a Service Provider (SP) in a Federated SSO model.

17. A user's equipment (UE) usable by a user with a subscription in a telecommunication network, and arranged to access a telecommunication service network (SN) through an access network (WLAN), the user's equipment (UE) having:

- means for carrying out (S-25) an authentication procedure (SIM-based; AKA; EAP) to authenticate the user with a core network (CN), where the user holds the subscription, through the access network (WLAN); and

- means for computing at least one secret user's key (K_C) usable as cryptographic material;

and **characterised by** comprising:

- means (S-252) for deriving from the cryptographic material a user's shared key (SSO_key-2) intended for SSO purposes;

- a repository for storing the user's shared key (SSO_key-2); and

- means for confirming (S-32, S-33) the user's shared key (SSO_key-2) stored at the user's equipment towards an entity (SAAN, SSO_SM) in the service network (SN).

18. The user's equipment of claim 17, wherein the means for confirming (S-32, S-33) includes means for downloading an SSO plug-in from an entity (SAAN, SSO_SM) in the service network (SN), the SSO plug-in running for confirming back the user's shared key.

19. The user's equipment of claim 17, wherein the means for confirming (S-32, S-33) includes means for processing the

user's shared key (SSO_key-2) to obtain a key code (MAC(SSO_key-2)) to be transmitted to an entity (SAAN, SSO_SM) in the service network (SN).

20. The user's equipment of claim 17, further comprising means for receiving an SSO cookie from an entity (SAAN, SSO_SM) in the service network, the SSO cookie to be included in all further service requests from the user's equipment as an SSO token.

21. A method for supporting Single Sign-On services for a user with a user's equipment (UE) arranged for accessing a telecommunication core network (CN) and service network (SN) through an access network (WLAN), the user being identified as subscriber of the telecommunication core network (CN) when accessing the access network (WLAN), the method comprising the steps of:

- carrying out (S-25) an authentication procedure for the user between the core network (CN) and the user's equipment (UE);

- computing at an entity (HLR, AUC, AG) of the core network (CN) at least one secret user's key (K_C) usable as cryptographic material; and

- computing at the user's equipment (UE) at least one secret user's key (K_C) usable as cryptographic material;

and **characterised by** including the steps of:

- deriving (S-251) a first user's key (SSO_key-1) intended for SSO purposes from the cryptographic material at an entity (AG) of the core network (CN);

- deriving (S-252) a second user's key (SSO_key-2) intended for SSO purposes from the cryptographic material at the user's equipment (UE);

- creating (S-301) a master session for the user at an entity (SAAN, SSO_SM) in the service network, the master session comprising a user's identifier and the first user's key (SSO_key-1);

- confirming (S-32, S-33) the second user's shared key (SSO_key-2) stored at the user's equipment towards the entity (SAAN, SSO_SM) in the service network (SN);

- verifying (S-34) whether the second user's shared key (SSO_key-2) matches the first user's shared key (SSO_key-1) for the user at the entity (SAAN, SSO_SM) in the service network (SN); and

- granting (S-35, S-36, S-37) access to the requested service in the service network (SN) on matching the first and second user's shared keys.

22. The method of claim 21, wherein the step of verifying (S-34) the matching of the first and second user's shared keys further includes a step of creating a service session to index the master session, this service session intended as a token of a successful SSO authentication.

23. The method of claim 22, further including a step of generating an SSO cookie to be submitted to the user's equipment, the SSO cookie comprising the service session.

24. The method of claim 23, further comprising a step of verifying whether an active service session is indicated in the request from the user's equipment.

25. The method of claim 21, wherein the step of confirming (S-32, S-33) the second user's shared key (SSO_key-2)

stored at the user's equipment, includes a step of downloading an SSN plug-in from an entity (SAAN, SSO_SM) in the service network (SN), the SSO plug-in running for confirming back the user's shared key (SSO_key-2).

26. The method of claim 21, wherein the step of confirming (S-32, S-33) the second user's shared key (SSO_key-2) stored at the user's equipment, includes a step of processing the user's shared key (SSO_key-2) to obtain a key code (MAC(SSO_key-2)) to be transmitted to an entity (SAAN, SSO_SM) in the service network (SN).

27. The method of claim 26, wherein the step of verifying (S-34) whether the second user's shared key (SSO_key-2) matches the first user's shared key (SSO_key-1) includes a step of processing at an entity (SAAN, SSO_SM) of the service network (SN) the first user's shared key (SSO_key-1) to obtain a first key code (MAC(SSO_key-1)) to be matched against a second key code (MAC(SSO_key-2)) originated from the user's equipment.

28. The method of claim 21, wherein the step of creating (S-301) a master session for the user at the entity (SAAN, SSO_SM) in the service network includes a step of receiving the first user's key (SSO_key-1) from an entity (AG) of the core network (CN).

29. The method of claim 21, wherein the step of creating (S-301) a master session for the user at the entity (SAAN, SSO_SM) in the service network includes a step of initiating an access session (S-29) when the user accesses the access network.